

ON SYSTEMS OF EQUATIONS IN FREE ABELIAN GROUPS

ANTON MENSHOV

ABSTRACT. In this paper we study the asymptotic probability that a random system of equations in free abelian group \mathbb{Z}^m of rank m is solvable. Denote $SAT(\mathbb{Z}^m, k, n)$ and $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ the sets of all systems of n equations in k variables in the group \mathbb{Z}^m solvable in \mathbb{Z}^m and \mathbb{Q}^m respectively. We show that asymptotic density of the set $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ is equal to 1 for $n \leq k$, and is equal to 0 for $n > k$. For $n < k$ we give nontrivial estimates for upper and lower asymptotic densities of the set $SAT(\mathbb{Z}^m, k, n)$. When $n > k$ the set $SAT(\mathbb{Z}^m, k, n)$ is negligible. Also for $n \leq k$ we provide some connection between asymptotic density of the set $SAT(\mathbb{Z}^m, k, n)$ and sums over full rank matrices involving their greatest divisors.

1. INTRODUCTION

In finite group theory the idea of genericity can be traced to works of Erdős and Turan [1] and Dixon [2]. Nowadays it is an area of active research. In geometric group theory the generic approach is due to Gromov [3, 4, 5] and is associated with random walks on groups.

Recently, a host of papers appeared on generic properties of individual groups. We mention here, in particular, results on generic properties of one-relator groups [6, 7] and averaged Dehn functions [8, 9].

Gilman, Myasnikov and Roman'kov studied satisfiability of random equations in free abelian and finitely generated nilpotent groups [10] and in free groups [11]. Probability of a homogeneous equation in a surface group to have solutions is studied in [12].

In this paper we study satisfiability of random systems of equations in free abelian groups of finite rank and extend corresponding results obtained in [10] for equations.

Denote $SAT(\mathbb{Z}^m, k, n)$ and $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ the sets of all systems of n equations in k variables in the group \mathbb{Z}^m solvable in \mathbb{Z}^m and \mathbb{Q}^m respectively. We study asymptotic density of the sets above with respect to the natural stratification of the group \mathbb{Z}^m with balls corresponding to the uniform norm $\|\cdot\|_\infty$ of Euclidean space \mathbb{R}^m . In the sequel we treat \mathbb{Z}^m and its subgroups as integer lattices in \mathbb{R}^m .

Key words and phrases. free abelian groups, equations in groups, asymptotic density, Ehrhart quasipolynomials.

In Section 3, using the asymptotics for the number of integral matrices of fixed rank [14], we show in theorem 3.2 that the set $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ is generic if $n \leq k$, and negligible if $n > k$.

In Section 4 we recall some basic notions concerning lattice points counting in rational polytopes and extend inequality [18, Theorem 6] derived for coefficients of Ehrhart polynomials to Ehrhart quasipolynomials (see theorem 4.5). Using this inequality, in theorem 5.6 we establish connection between asymptotic density of the set $SAT(\mathbb{Z}^m, k, n)$ and sums of inverse greatest divisors over full rank matrices. Based on this result, we make a conjecture 5.7 concerning asymptotic density of the set $SAT(\mathbb{Z}^m, n, n)$. In theorem 5.10 we give nontrivial estimates for upper and lower asymptotic densities of the set $SAT(\mathbb{Z}^m, k, n)$. Namely, we show that for $n < k$ this densities lie in the interval from $\left(\prod_{j=k-n+1}^k \zeta(j)\right)^{-1}$ to $\left(\frac{\zeta(k+m)}{\zeta(k)}\right)^n$, where $\zeta(s)$ is Riemann zeta-function.

2. PRELIMINARIES

2.1. Asymptotic density. A *stratification* of a countable set T is a sequence $\{T_r\}_{r \in \mathbb{N}}$ of non-empty finite subsets T_r whose union is T . Stratifications are often specified by length functions. A *length function* on T is a map $l : T \rightarrow \mathbb{N}$ from T to the nonnegative integers \mathbb{N} such that the inverse image of every integer is finite. The corresponding spherical and ball stratifications are formed by *spheres* $S_r = \{x \in T \mid l(x) = r\}$ and *balls* $B_r = \{x \in T \mid l(x) \leq r\}$.

Definition 2.1. The asymptotic density of $M \subset T$ with respect to a stratification $\{T_r\}$ is defined to be

$$\rho(M) = \lim_{r \rightarrow \infty} \rho_r(M), \quad \text{where} \quad \rho_r(M) = \frac{|M \cap T_r|}{|T_r|}$$

when the limit exists. Otherwise, we use the limits

$$\bar{\rho}(M) = \limsup_{r \rightarrow \infty} \rho_r(M), \quad \underline{\rho}(M) = \liminf_{r \rightarrow \infty} \rho_r(M),$$

and call them upper and lower asymptotic densities respectively.

M is said to be *generic* in T with respect to the stratification $\{T_r\}_{r \in \mathbb{N}}$ if $\rho(M) = 1$ and *negligible* if $\rho(M) = 0$. A property of elements of T is generic if it holds on a generic subset.

Asymptotic density is one of the tools for measuring sets in infinite groups (see [13] for details).

Let \mathbb{Z}^m be a free abelian group of rank m . We identify \mathbb{Z}^m with the standard integer lattice in Euclidean space \mathbb{R}^m . We assume that \mathbb{R}^m is equipped with the uniform norm defined for $v = (v_1, \dots, v_m)$ by the formula

$$\|v\|_{\infty} = \max_i \{|v_i|\}.$$

This norm induces the length function $\|\cdot\|_\infty : \mathbb{Z}^m \rightarrow \mathbb{N}$ with balls

$$B_r^m = \{v \in \mathbb{Z}^m \mid \|v\|_\infty \leq r\}.$$

Further we will compute asymptotic density of some subsets in free abelian groups with respect to the given ball stratification.

2.2. Equations in groups. An equation $u = 1$ in k variables over a group G is an expression of the form

$$g_0 x_{i_1}^{m_1} g_1 \dots x_{i_n}^{m_n} g_n = 1,$$

where each coefficient g_j is a group element, each exponent m_j is an integer, and each x_{i_j} is taken from an alphabet of variables, $X = \{x_1, \dots, x_k\}$. In this case, the free product $G_X = F(X) * G$ is the space of all equations in variables X and coefficients in G . A solution of $u = 1$ in G is an assignment $x_j \rightarrow h_j \in G$ such that $g_0 h_{i_1}^{m_1} g_1 \dots h_{i_n}^{m_n} g_n = 1$. Denote by $SAT(G, K)$ the set of all equations from G_X which have a solution in G (*satisfiable* equations).

Since we study equations in free abelian groups, we will use additive notation throughout. In line with this we will write equation as

$$(2.1) \quad \gamma_1 \mathbf{x}_1 + \dots + \gamma_k \mathbf{x}_k = \mathbf{b},$$

where $\gamma_j \in \mathbb{Z}$ and $\mathbf{b} \in \mathbb{Z}^m$ are fixed, and $\mathbf{x}_j = (x_{j1}, \dots, x_{jm})$ are variables.

System

$$(2.2) \quad \begin{cases} \gamma_{11} \mathbf{x}_1 + \dots + \gamma_{1k} \mathbf{x}_k = \mathbf{b}_1, \\ \vdots \\ \gamma_{n1} \mathbf{x}_1 + \dots + \gamma_{nk} \mathbf{x}_k = \mathbf{b}_n, \end{cases}$$

of n equations of the form (2.1) will be written as

$$(2.3) \quad AX = B,$$

where

$$A = (\gamma_{ij}) \in \mathbb{Z}^{nk}, \quad B = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix} \in \mathbb{Z}^{nm}, \quad \text{and} \quad X = \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_k \end{pmatrix}.$$

It is natural to consider two equations as essentially the same if one can be transformed into the other by applying identities of the variety of abelian groups. So the natural space of equations in variables $X = \{x_1, \dots, x_k\}$ over a free abelian group \mathbb{Z}^m is the direct product $A(X) \times \mathbb{Z}^m \simeq \mathbb{Z}^{k+m}$ of a free abelian group $A(X)$ with basis X and group \mathbb{Z}^m . By $G_{X,n}$ we denote the space of all systems of n equations from G_X and $\mathbb{Z}^{n(k+m)}$ is a natural choice for it. We denote $SAT(G, k, n)$ the set of all systems from $G_{X,n}$ solvable in G . Systems from $\mathbb{Z}_{X,n}^m$ solvable in \mathbb{Q}^m will be denoted by $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$.

Observe, that in (2.3) different coordinates of variables are independent from each other, so the following obvious lemma holds.

Lemma 2.2. *A system $AX = B$ of the form (2.3) is solvable in $\mathbb{Z}^m(\mathbb{Q}^m)$ if and only if systems $Ax = B_i$ are solvable over $\mathbb{Z}(\mathbb{Q})$ for any $i = 1, \dots, m$, where B_i is the i -th column of the matrix B .*

If $X_i = (x_{1i}, \dots, x_{ki})^T$ is a solution of $Ax = B_i$, then $X = (X_1, \dots, X_m)$ is a solution of $AX = B$.

3. SYSTEMS SOLVABLE IN \mathbb{Q}^m

In this section we will compute asymptotic density of the set $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ of all systems of n equations in k variables in \mathbb{Z}^m solvable in \mathbb{Q}^m .

Consider a system of linear diophantine equations $Ax = b$ with $A \in \mathbb{Z}^{nk}, b \in \mathbb{Z}^n$. According to Kronecker-Capelli theorem the system above has solution over \mathbb{Q} if and only if the rank of its coefficient matrix A is equal to the rank of augmented matrix $(A|b)$.

We state here the main result of [14] where the asymptotics for the number of integral matrices of fixed rank is derived. Denote

$$V_{n,k,s}(\mathbb{Z}) = \{A \in \mathbb{Z}^{nk} \mid \text{rank}(A) = s\},$$

$$N(r; n, k, s) = |\{A \in V_{n,k,s}(\mathbb{Z}) \mid \|A\|_2 < r\}|,$$

where $\|A\|_2 = \sqrt{(\sum_{i,j} a_{ij}^2)}$.

Theorem 3.1 (Katznelson [14]). *For $k \geq n > s \geq 1$ and as r tends to infinity:*

- (1) for $n < k$, $N(r; n, k, s) = \alpha(n, k, s)r^{ks} + O(r^{ks-1})$.
- (2) for $n = k$, $N(r; k, k, s) = \beta(k, s)r^{ks} \log r + O(r^{ks})$.

Observe, that the growth rate of $N(r; n, k, s)$ doesn't change if we replace the norm $\|\cdot\|_2$ by $\|\cdot\|_\infty$. Denote

$$N(r; n, k, s)_\infty = |\{A \in V_{n,k,s}(\mathbb{Z}) \mid \|A\|_\infty < r\}|.$$

It is easy to see that

$$\frac{1}{\sqrt{nk}} \|A\|_2 \leq \|A\|_\infty \leq \|A\|_2$$

and

$$N(r; n, k, s) \leq N(r; n, k, s)_\infty \leq N(r\sqrt{nk}; n, k, s).$$

Therefore for $s = 1, \dots, n-1$

$$(3.1) \quad \rho(V_{n,k,s}(\mathbb{Z})) = \lim_{r \rightarrow \infty} \frac{N(r; n, k, s)_\infty}{(2r+1)^{nk}} = 0$$

which implies that $\rho(V_{n,k,n}(\mathbb{Z})) = 1$, i.e., asymptotically almost all $n \times k$ matrices have full rank.

Theorem 3.2. *The set $SAT_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$ is generic if $n \leq k$ and negligible if $n > k$.*

Proof. Denote $B_r = B_r^{n(k+m)}$. Consider the set

$$S_1 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid \text{rank}(A) = n\}$$

of all systems $AX = B$ of the form (2.3) for $n \leq k$. All systems from S_1 are solvable in \mathbb{Q}^m , hence the following inclusion holds $S_1 \subset \text{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$. Consider the projection $\pi_1 : \mathbb{Z}^{n(k+m)} \rightarrow \mathbb{Z}^{nk}$, defined by $\pi_1(A|B) = A$. Observe, that

$$\pi_1(S_1 \cap B_r) = V_{n,k,n}(\mathbb{Z}) \cap \pi_1(B_r)$$

and each preimage contains $(2r+1)^{nm}$ elements. Hence

$$\frac{|\pi_1(S_1 \cap B_r)|}{(2r+1)^{nk}} = \rho_r(V_{n,k,n}(\mathbb{Z}))$$

and

$$\rho_r(S_1) = \frac{|S_1 \cap B_r|}{|B_r|} = (2r+1)^{nm} \frac{|\pi_1(S_1 \cap B_r)|}{(2r+1)^{n(k+m)}} = \rho_r(V_{n,k,n}(\mathbb{Z})).$$

Therefore $\rho(S_1) = \rho(V_{n,k,n}(\mathbb{Z})) = 1$, which implies that for $n \leq k$

$$\rho(\text{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 1.$$

Next consider the set

$$S_2 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid \text{rank}(A|B_1) < k+1\}$$

of all systems $AX = B$ of the form (2.3) for $n > k$, where B_1 is the first column of the matrix B . According to lemma 2.2 solvability of the system $AX = B$ in \mathbb{Q}^m implies solvability of the system $Ax = B_1$ over \mathbb{Q} , so $\text{rank}(A|B_1) < k+1$ since $n > k$. Thus the following inclusion holds $\text{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n) \subset S_2$. Consider the projection $\pi_2 : \mathbb{Z}^{n(k+m)} \rightarrow \mathbb{Z}^{n(k+1)}$, defined by $\pi_2(A|B) = (A|B_1)$. Observe, that

$$\pi_2(S_2 \cap B_r) = \pi_2(B_r) \setminus (V_{k+1,n,k+1}(\mathbb{Z}) \cap \pi_2(B_r))$$

and each preimage contains $(2r+1)^{n(m-1)}$ elements. Hence

$$\frac{|\pi_2(S_2 \cap B_r)|}{(2r+1)^{n(k+1)}} = 1 - \rho_r(V_{k+1,n,k+1}(\mathbb{Z}))$$

and

$$\rho_r(S_2) = \frac{|S_2 \cap B_r|}{|B_r|} = (2r+1)^{n(m-1)} \frac{|\pi_2(S_2 \cap B_r)|}{(2r+1)^{n(k+m)}} = 1 - \rho_r(V_{k+1,n,k+1}(\mathbb{Z})).$$

Therefore $\rho(S_2) = 1 - \rho(V_{k+1,n,k+1}(\mathbb{Z})) = 0$, which implies that for $n > k$

$$\rho(\text{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)) = 0.$$

□

Corollary 3.3. *The set $\text{SAT}(\mathbb{Z}^m, k, n)$ is negligible if $n > k$.*

Proof. Since $\text{SAT}(\mathbb{Z}^m, k, n) \subset \text{SAT}_{\mathbb{Q}^m}(\mathbb{Z}^m, k, n)$, it follows that for $n > k$ $\rho(\text{SAT}(\mathbb{Z}^m, k, n)) = 0$. □

4. LATTICE POINTS IN RATIONAL POLYTOPES

Counting lattice points in the integral dilates of a subset of Euclidean space \mathbb{R}^d is a well known problem. For rational polytopes this problem has been studied in the 1960s by the French mathematician Eugène Ehrhart. These results may be useful when computing asymptotic densities in free abelian groups (see, for example, [19]). Detailed survey of further results can be found in [15] (see also [16]). We recall some basic notions first. A *convex polytope* in \mathbb{R}^d is a finite intersection of closed half-spaces, i.e.,

$$\mathcal{P} = \{\mathbf{x} \in \mathbb{R}^d \mid A\mathbf{x} \leq b\}, \text{ where } A \in \mathbb{R}^{md}, b \in \mathbb{R}^m.$$

This definition is called the *hyperplane description* of \mathcal{P} . Also any bounded convex polytope in \mathbb{R}^d has the *vertex description* and could be presented as the convex hull of finitely many points in \mathbb{R}^d . This vertex description of a polytope is equivalent to the hyperplane description.

The *dimension* of a polytope \mathcal{P} is the dimension of the affine space

$$\text{span } \mathcal{P} = \{\mathbf{x} + \lambda(\mathbf{y} - \mathbf{x}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{P}, \lambda \in \mathbb{R}\}$$

spanned by \mathcal{P} . If \mathcal{P} has dimension d , we use the notation $\dim \mathcal{P} = d$ and call \mathcal{P} a d -polytope.

A bounded convex polytope \mathcal{P} is called *integral* if all of its vertices have integral coordinates, and \mathcal{P} is called *rational* if all of its vertices have rational coordinates. We will call the least common multiple of the denominators of the coordinates of the vertices of \mathcal{P} the *denominator* of \mathcal{P} .

For $t \in \mathbb{Z}^+$ denote $t\mathcal{P} = \{t\mathbf{x} \mid \mathbf{x} \in \mathcal{P}\}$ the t^{th} dilate of \mathcal{P} . We denote the *lattice-point enumerator* for the t^{th} dilates of \mathcal{P} by

$$L_{\mathcal{P}}(t) = |t\mathcal{P} \cap \mathbb{Z}^d|.$$

We define the *Ehrhart series* of \mathcal{P} as the generating function of $L_{\mathcal{P}}(t)$

$$\text{Ehr}_{\mathcal{P}}(z) = \sum_{t \geq 0} L_{\mathcal{P}}(t) z^t.$$

Here we assume that $L_{\mathcal{P}}(0) = 1$.

By $\binom{n}{k}$ we denote the *binomial coefficient*, defined through

$$(4.1) \quad \binom{n}{k} = \frac{n(n-1) \dots (n-k+1)}{k!}$$

for $n \in \mathbb{C}$, $k \in \mathbb{Z}^+$.

The following theorem states some known results concerning lattice points in integral polytopes [15, theorems 3.8, 3.12 and lemmas 3.13, 3.14].

Theorem 4.1. *If \mathcal{P} is an integral convex d -polytope, then*

- (1) $\text{Ehr}_{\mathcal{P}}(z) = \frac{h_d z^d + \dots + h_1 z + 1}{(1-z)^{d+1}}$ with $h_i \in \mathbb{N}$,
- (2) $L_{\mathcal{P}}(t) = \binom{t+d}{d} + h_1 \binom{t+d-1}{d} + \dots + h_{d-1} \binom{t+1}{d} + h_d \binom{t}{d}$ is a polynomial in t of degree d .

$L_{\mathcal{P}}(t)$ is called the *Ehrhart polynomial* of \mathcal{P} .

Some coefficients of $L_{\mathcal{P}}(t) = c_d t^d + \cdots + c_1 t + c_0$ have geometric interpretation. For example, the leading coefficient c_d is equal to d -dimensional volume of \mathcal{P} [15, corollary 3.20], which implies that

$$(4.2) \quad \text{vol}(\mathcal{P}) = \frac{1}{d!} (h_d + \cdots + h_1 + 1).$$

It is also known that $c_0 = 1$ [15, corollary 3.15].

We recall that a *quasipolynomial* Q is an expression of the form $Q(t) = c_n(t)t^n + \cdots + c_1(t)t + c_0(t)$, where c_0, \dots, c_n are periodic functions in t and c_n is not the zero function. The *degree* of Q is n , and the least common period of c_0, \dots, c_n is the *period* of Q . Alternatively, for a quasipolynomial Q , there exist a positive integer k and polynomials p_0, p_1, \dots, p_{k-1} such that $Q(t) = p_i(t)$ if $t \equiv i \pmod{k}$. The minimal such k is the period of Q .

Results of the theorem 4.1 can be extended to rational polytopes [15, theorem 3.23, ex. 3.25].

Theorem 4.2. *If \mathcal{P} is a rational convex d -polytope with the denominator p , then*

- (1) $\text{Ehr}_{\mathcal{P}}(z) = \frac{\sum_{i=0}^{d(p+1)-1} h_i z^i}{(1-z^p)^{d+1}}$ with $h_i \in \mathbb{N}$,
- (2) $L_{\mathcal{P}}(t)$ is a quasipolynomial in t of degree d and its period divides p .

$L_{\mathcal{P}}(t)$ is called the *Ehrhart quasipolynomial* of \mathcal{P} .

We note that there is an algorithm by Alexander Barvinok to compute Ehrhart quasipolynomials. Barvinok's algorithm is polynomial in fixed dimension, it has been implemented in the software package **LattE** [17].

We will need an explicit formula for Ehrhart quasipolynomials, similar to one specified in theorem 4.1 for Ehrhart polynomials.

Lemma 4.3. *In notations of the theorem 4.2*

$$L_{\mathcal{P}}(t) = f_j(t) \quad \text{if } t \equiv j \pmod{p}$$

where

$$f_j(t) = h_j \binom{t+d}{d} + h_{p+j} \binom{t+d-1}{d} + \cdots + h_{dp+j} \binom{t}{d}.$$

Proof.

$$\begin{aligned}
\text{Ehr}_{\mathcal{P}}(z) &= \frac{\sum_{i=0}^d \sum_{j=0}^{p-1} h_{ip+j} z^{ip+j}}{(1-z^p)^{d+1}} \\
&= \left(\sum_{i=0}^d \sum_{j=0}^{p-1} h_{ip+j} z^{ip+j} \right) \sum_{t \geq 0} \binom{t+d}{d} z^{tp} \\
&= \sum_{i=0}^d \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq 0} \binom{t+d}{d} z^{ip+j+tp} \\
&= \sum_{i=0}^d \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq i} \binom{t+d-i}{d} z^{pt+j}.
\end{aligned}$$

In all infinite sums we can start the index t with 0. Hence

$$\begin{aligned}
\text{Ehr}_{\mathcal{P}}(z) &= \sum_{i=0}^d \sum_{j=0}^{p-1} h_{ip+j} \sum_{t \geq 0} \binom{t+d-i}{d} z^{pt+j} \\
&= \sum_{j=0}^{p-1} \sum_{t \geq 0} \left(\sum_{i=0}^d h_{ip+j} \binom{t+d-i}{d} \right) z^{pt+j} \\
&= \sum_{j=0}^{p-1} \sum_{t \geq 0} f_j(t) z^{pt+j}.
\end{aligned}$$

□

For Ehrhart quasipolynomials $L_{\mathcal{P}}(t) = c_d(t)t^d + \dots + c_1(t)t + c_0(t)$ the leading coefficient $c_d(t)$ is equal to d -dimensional volume of \mathcal{P} and $c_0(t) = 1$. So c_d and c_0 are constants. This implies the formula similar to (4.2)

$$(4.3) \quad \text{vol}(\mathcal{P}) = \frac{1}{d!} (h_j + h_{p+j} + \dots + h_{dp+j}),$$

for $j = 0, \dots, p-1$.

The coefficients of Ehrhart polynomials are very special, see [20] for example. We will be interested in the following inequality.

Theorem 4.4 (Betke, McMullen [18]). *If \mathcal{P} is an integral convex d -polytope with Ehrhart polynomial $L_{\mathcal{P}}(t) = c_d t^d + \dots + c_1 t + 1$, then*

$$c_r \leq (-1)^{d-r} s(d, r) c_d + (-1)^{d-r-1} \frac{s(d, r+1)}{(d-1)!} \quad \text{for } r = 1, \dots, d-1,$$

where $s(i, j)$ denote the Stirling numbers of the first kind.

We recall that Stirling numbers of the first kind $s(n, k)$ are defined through

$$(4.4) \quad [x]_n = x(x-1) \dots (x-n+1) = \sum_{k=0}^n s(n, k) x^k.$$

Now we extend the inequality above to rational polytopes.

Theorem 4.5. *If \mathcal{P} is a rational convex d -polytope with the denominator p and Ehrhart quasipolynomial $L_{\mathcal{P}}(t) = c_d t^d + c_{d-1}(t)t^{d-1} + \cdots + c_1(t)t + 1$, then*

$$|c_r(t)| \leq |s(d+1, r+1)|c_d \quad \text{for } r = 1, \dots, d-1, \quad t \in \mathbb{Z}^+$$

Proof. For arbitrary polynomial $g(x)$ by $g(x)|_i$ we denote the coefficient of x^i in $g(x)$.

According to lemma 4.3 we have $L_{\mathcal{P}}(t) = f_j(t)$ if $t \equiv j \pmod{p}$, where

$$f_j(t) = \sum_{i=0}^d h_{ip+j} \binom{t+d-i}{d}.$$

Then

$$c_r(j) = f_j(t)|_r = \left(\sum_{i=0}^d h_{ip+j} \binom{t+d-i}{d} \right) \Big|_r = \sum_{i=0}^d h_{ip+j} \left(\binom{t+d-i}{d} \right) \Big|_r.$$

It is easy to see that for $i = 1, \dots, d$

$$\left| \binom{t+d-i}{d} \right|_r \leq \left(\binom{t+d}{d} \right) \Big|_r.$$

From (4.3), since $h_i \in \mathbb{N}$, it follows that for $j = 0, \dots, p-1$

$$\begin{aligned} |c_r(j)| &= |f_j(t)|_r \\ &\leq \sum_{i=0}^d h_{ip+j} \left| \binom{t+d-i}{d} \right|_r \\ &\leq \sum_{i=0}^d h_{ip+j} \left(\binom{t+d}{d} \right) \Big|_r \\ &= \left(\binom{t+d}{d} \right) \Big|_r (h_j + h_{p+j} + \cdots + h_{dp+j}) \\ &= \left(\binom{t+d}{d} \right) \Big|_r d! \operatorname{vol}(\mathcal{P}) = |s(d+1, r+1)|c_d. \end{aligned}$$

□

Let $\mathbf{w}_1, \dots, \mathbf{w}_d$ be lineary independent vectors in \mathbb{R}^d . The set

$$\Lambda = \Lambda(\mathbf{w}_1, \dots, \mathbf{w}_d) = \{\alpha_1 \mathbf{w}_1 + \cdots + \alpha_d \mathbf{w}_d \mid \alpha_i \in \mathbb{Z}\}$$

is called the *lattice* with basis $\{\mathbf{w}_1, \dots, \mathbf{w}_d\}$. The number

$$d(\Lambda) = |\det(\mathbf{w}_1, \dots, \mathbf{w}_d)|$$

is called the *determinant* of the lattice.

A convex polytope \mathcal{P} is called *lattice polytope* (with respect to the lattice Λ) if all of its vertices belongs to Λ .

We note that results of this section remains true if we replace the standard integer lattice \mathbb{Z}^d by an arbitrary lattice $\Lambda(\mathbf{w}_1, \dots, \mathbf{w}_d)$. Indeed, consider the matrix $A = (\mathbf{w}_1, \dots, \mathbf{w}_d)$ formed by \mathbf{w}_i as columns and let ψ be the linear transformation corresponding to A . Then $\Lambda = \psi(\mathbb{Z}^d)$ and $\mathbb{Z}^d = \psi^{-1}(\Lambda)$. If \mathcal{P} is a rational d -polytope with respect to the basis $\{\mathbf{w}_1, \dots, \mathbf{w}_d\}$, then $\psi^{-1}(\mathcal{P})$ is a rational d -polytope with respect to the standard basis of \mathbb{R}^d and

$$L_{\mathcal{P}, \Lambda}(t) = |\{t\mathcal{P} \cap \Lambda\}| = \left| \{t\psi^{-1}(\mathcal{P}) \cap \mathbb{Z}^d\} \right|.$$

Given that $\text{vol}(\mathcal{P}) = |\det(A)|\text{vol}(\psi^{-1}(\mathcal{P}))$ we get that the leading coefficient of $L_{\mathcal{P}, \Lambda}(t)$ is equal to $\frac{\text{vol}(\mathcal{P})}{d(\Lambda)}$.

5. SYSTEMS SOLVABLE IN \mathbb{Z}^m

Let $M \in \mathbb{Z}^{nk}$ ($n \leq k$) and $\text{rank}(M) = n$, then by $\text{gcd}(M)$ we denote the *greatest divisor* of M , defined as the greatest common divisor of the determinants of M . The determinants of a matrix are, of course, the determinants of the greatest square matrices contained in it. A matrix M is called *unimodular* if $\text{gcd}(M) = 1$.

First we recall some classical criterions telling whether a linear diophantine systems of the form

$$(5.1) \quad Ax = b \quad \text{with } A \in \mathbb{Z}^{nk}, b \in \mathbb{Z}^n,$$

has integral solution.

Theorem 5.1 (Smith [21]). *Let $Ax = b$ be a system of the form (5.1) with $\text{rank}(A) = n$. Then the system has integral solution if and only if the greatest divisors of its augmented and unaugmented matrices are equal.*

We also mention a criterion due to Van der Waerden.

Theorem 5.2 (Van der Waerden). *A system $Ax = b$ of the form (5.1) has integral solution if and only if for every $v \in \mathbb{Q}^n$ such that $vA \in \mathbb{Z}^k$, $(v, b) \in \mathbb{Z}$.*

However, we will use other criterion wich allows us to apply results of Section 4.

For $n \leq k$ consider a system from $\mathbb{Z}_{X,n}^m$ of the form

$$(5.2) \quad AX = B \quad \text{with } A \in \mathbb{Z}^{nk}, B \in \mathbb{Z}^{nm}.$$

Denote A_i and B_j the columns of A and B respectively, and let $H_A = \langle A_1, \dots, A_k \rangle \leq \mathbb{Z}^n$ be the subgroup generated by the columns of A . Then the following obvious lemma holds.

Lemma 5.3. *A system $AX = B$ of the form (5.2) is solvable in \mathbb{Z}^m if and only if $B_i \in H_A$ for every $i = 1, \dots, m$.*

If $\text{rank}(A) = n$ then H_A is of finite index, thus H_A is a n -dimensional lattice in \mathbb{R}^n with determinant $d(H_A) = |\mathbb{Z}^n : H_A| = \gcd(A)$. Therefore

$$|\{B_r^n \cap H_A\}| = |\{rB_1^n \cap H_A\}| = L_{B_1^n, H_A}(r)$$

is Ehrhart quasipolynomial for B_1^n , which further will be denoted by $L_A(r)$. Consider the sum

$$(5.3) \quad S_{m,k,n}(r) = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} L_A^m(r).$$

According to lemma 5.3 this sum describes the number of solvable systems of the form (5.2) with $\text{rank}(A) = n$ in the ball $B_r^{n(k+m)}$. Let

$$L_A(t) = c_{A,n}t^n + c_{A,n-1}(t)t^{n-1} + \cdots + c_{A,1}(t)t + 1,$$

$$L_A^m(r) = \sum_{i=0}^{mn} \alpha_{A,i} r^i,$$

then $S_{m,k,n}(r)$ can be presented as

$$S_{m,k,n}(r) = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \sum_{i=0}^{mn} \alpha_{A,i} r^i = \sum_{i=0}^{mn} \left(\sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \alpha_{A,i} \right) r^i = \sum_{i=0}^{mn} s_{m,k,n,i}(r) r^i.$$

It is easy to see that $\alpha_{A,0} = 1$ and

$$\alpha_{A,mn} = c_{A,n}^m = \left(\frac{\text{vol}(B_1^n)}{d(H_A)} \right)^m = 2^{mn} \gcd(A)^{-m},$$

so

$$s_{m,k,n,mn}(r) = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \alpha_{A,mn} = 2^{mn} \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \gcd(A)^{-m}.$$

Lemma 5.4. *As r tends to infinity $s_{m,k,n,mn}(r) = O(r^{nk})$.*

Proof. Observe, that

$$\begin{aligned} s_{m,k,n,mn}(r) &= 2^{mn} \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \gcd(A)^{-m} \\ &\leq 2^{mn} \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} 1 \\ &\leq 2^{mn} |B_r^{nk}| = 2^{mn} (2r+1)^{nk}. \end{aligned}$$

□

The following lemma shows that $r^{mn} s_{m,k,n,mn}(r)$ makes a major contribution to the sum $S_{m,k,n}(r)$ from the asymptotic point of view.

Lemma 5.5. $\lim_{r \rightarrow \infty} \frac{s_{m,k,n,i}(r)r^i}{r^{n(k+m)}} = 0$ for $i = 0, \dots, mn - 1$.

Proof. The case $i = 0$ is obvious since $\alpha_{A,0} = 1$.

According to the theorem 4.5 for $r = 1, \dots, n - 1$

$$|c_{A,r}(t)| \leq \max_i \{|s(n+1, i)|\} c_{A,n},$$

then for any sum of the form

$$(5.4) \quad \Omega(r) = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} c_{A,i_1}(r) \dots c_{A,i_s}(r), \quad \text{where } i_j \in \{1, \dots, n\}$$

we have $|\Omega(r)| \leq \beta s_{s,k,n,sn}(r)$, for some constant β , which doesn't depend on r . So $\Omega(r) = O(r^{nk})$. Any sum

$$s_{m,k,n,i}(r) = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \alpha_{A,i}$$

is a finite sum of the sums of the form (5.4), so it is also $O(r^{nk})$.

Statement of the lemma now follows from the fact that for any function $f(r) = O(r^{nk})$

$$\lim_{r \rightarrow \infty} \frac{f(r)r^i}{r^{n(k+m)}} = 0 \quad \text{if } i < mn.$$

□

Denote

$$F_{m,k,n}(r) = \frac{s_{m,k,n,mn}(r)}{2^{mn}} = \sum_{\substack{A \in B_r^{nk} \\ \text{rank}(A)=n}} \gcd(A)^{-m}.$$

We now establish a connection between $F_{m,k,n}(r)$ and asymptotic density of the set $SAT(\mathbb{Z}^m, k, n)$.

Theorem 5.6. $\rho(SAT(\mathbb{Z}^m, k, n)) = \rho$ if and only if $\lim_{r \rightarrow \infty} \frac{F_{m,k,n}(r)}{(2r)^{nk}} = \rho$.

Proof. If asymptotic density of the set $SAT(\mathbb{Z}^m, k, n)$ exists, then according to (3.1) only systems with full rank matrices contribute to asymptotic density, so

$$\lim_{r \rightarrow \infty} \frac{S_{m,k,n}(r)}{|B_r^{n(k+m)}|} = \rho.$$

According to lemma 5.5 only the leading term of $S_{m,k,n}(r)$ contribute to the limit above, hence

$$\rho = \lim_{r \rightarrow \infty} \frac{s_{m,k,n,mn}(r)r^{mn}}{|B_r^{n(k+m)}|} = \lim_{r \rightarrow \infty} \frac{s_{m,k,n,mn}(r)r^{mn}}{(2r)^{n(k+m)}} = \lim_{r \rightarrow \infty} \frac{F_{m,k,n}(r)}{(2r)^{nk}}.$$

Arguing as above one can show that the converse is true.

□

Now we consider the case when $n = k$ and $m = 1$. Then

$$(5.5) \quad F_{1,n,n}(r) = \sum_{\substack{A \in B_r^{nn} \\ \text{rank}(A)=n}} \frac{1}{|\det(A)|}.$$

In [22] asymptotics for the number of integral matrices of fixed determinant is derived. Let

$$V_{n,k} = \{M \in \mathbb{Z}^{nn} \mid \det(M) = k\},$$

$$N(r, V_{n,k}) = |\{M \in V_{n,k} \mid \|M\|_2 \leq r\}|,$$

then according to [22, example 1.6]

$$N(r, V_{n,k}) \sim c_{n,k} r^{n^2-n}.$$

If we assume that each value occurs (roughly) equally often, then

$$F_{1,n,n}(r) = O(r^{n^2-n} \ln(r)),$$

so

$$\lim_{r \rightarrow \infty} \frac{F_{1,n,n}(r)}{(2r)^{nn}} = 0$$

and $\rho(\text{SAT}(\mathbb{Z}, n, n)) = 0$. Since

$$\rho(\text{SAT}(\mathbb{Z}^{m+1}, n, n)) \leq \rho(\text{SAT}(\mathbb{Z}^m, n, n)),$$

then $\rho(\text{SAT}(\mathbb{Z}^m, n, n)) = 0$ for arbitrary m .

This allows us to formulate the following conjecture.

Conjecture 5.7. $F_{1,n,n}(r) = O(r^{n^2-n} \ln(r))$ and $\rho(\text{SAT}(\mathbb{Z}^m, n, n)) = 0$.

In the rest of this section we give some nontrivial estimates for upper and lower asymptotic densities of the set $\text{SAT}(\mathbb{Z}^m, k, n)$.

Denote $U_{n,k}$ the set of all $n \times k$ unimodular integer matrices. Below, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is Riemann zeta-function.

Asymptotic density of rectangular unimodular integer matrices is derived in [23].

Theorem 5.8 (Maze, Rosenthal, Wagner [23]).

- (1) $\rho(U_{n,k}) = \left(\prod_{j=k-n+1}^k \zeta(j) \right)^{-1}$ if $k > n \geq 1$,
- (2) $\rho(U_{n,n}) = 0$ if $n \geq 1$.

We note that [23] uses a slightly different notion of natural density in \mathbb{Z}^{nk} , which is nevertheless equivalent to our definition of asymptotic density with respect to balls stratification.

Theorem 5.8 allows us to bound lower asymptotic density of the set $\text{SAT}(\mathbb{Z}^m, k, n)$, since every system of the form (5.2) with unimodular matrix A is solvable in \mathbb{Z}^m . To bound upper asymptotic density we need to know asymptotic density of solvable equations in \mathbb{Z}^m .

Theorem 5.9 (Gilman, Myasnikov, Roman'kov [10]).

- (1) $\rho(\text{SAT}(\mathbb{Z}^m, k)) = \frac{\zeta(k+m)}{\zeta(k)}$ if $k \geq 2$,
- (2) $\rho(\text{SAT}(\mathbb{Z}^m, 1)) = 0$.

Now we are ready to prove the following theorem.

Theorem 5.10. *The following inequalities holds*

- (1) $\rho(U_{n,k}) \leq \underline{\rho}(\text{SAT}(\mathbb{Z}^m, k, n))$ if $k > n > 1$,
- (2) $\overline{\rho}(\text{SAT}(\mathbb{Z}^m, k, n)) \leq \rho(\text{SAT}(\mathbb{Z}^m, k))^n$ if $k \geq n > 1$.

Proof. Consider the set

$$S_1 = \{(A|B) \in \mathbb{Z}^{n(k+m)} \mid A \text{ is unimodular}\} \subset \text{SAT}(\mathbb{Z}^m, k, n)$$

when $k > n > 1$. It is easy to show that $\rho(S_1) = \rho(U_{n,k})$. Then

$$\rho(U_{n,k}) \leq \underline{\rho}(\text{SAT}(\mathbb{Z}^m, k, n)).$$

Next consider the set S_2 of all systems from $\mathbb{Z}_{X,n}^m$, where each equation is solvable. Clearly $\text{SAT}(\mathbb{Z}^m, k, n) \subset S_2$. Observe, that

$$\rho_r(S_2) = \rho_r(\text{SAT}(\mathbb{Z}^m, k))^n$$

and

$$\rho(S_2) = \lim_{r \rightarrow \infty} \rho_r(S_2) = \left(\lim_{r \rightarrow \infty} \rho_r(\text{SAT}(\mathbb{Z}^m, k)) \right)^n = \rho(\text{SAT}(\mathbb{Z}^m, k))^n.$$

Then

$$\overline{\rho}(\text{SAT}(\mathbb{Z}^m, k, n)) \leq \rho(\text{SAT}(\mathbb{Z}^m, k))^n.$$

□

ACKNOWLEDGEMENTS

The author would like to thank Professor V. A. Roman'kov for his valuable comments and suggestions.

REFERENCES

- [1] Erdos P., Turan P. *On some problems of statistical group theory I* // Z. Wahrscheinlichkeitstheorie verw. Geb., 1965, V. 4, P. 175–186
- [2] Dixon J. *The probability of generating the symmetric group* // Math. Z., 1969, V. 110, N. 3, P. 199–205.
- [3] Gromov M. *Hyperbolic Groups* // In: Essays in Group Theory, MSRI publ. 8, (1987), P. 75–263.
- [4] Gromov M. *Asymptotic invariants of infinite groups* // Geometric group theory, vol. 2 (Sussex, 1991), 1–295, London Math. Soc. Lecture Note Ser., vol. 182, Cambridge Univ. Press, Cambridge, 1993.
- [5] Gromov M. *Random walks in random groups* // Geom. Funct. Analysis, 2003, V. 13, P. 73–146.
- [6] Kapovich I., Schupp P. *Genericity, the Arzhantseva-Olshanskii method and the isomorphism problem for one-relator groups* // Math. Ann., 2005, V. 331, N. 1, P. 1–19.
- [7] Kapovich I., Schupp P. *Delzants T-invariant, one-relator groups and Kolmogorov complexity* // Comment. Math. Helv., 2005, V. 80, P. 911–933.

- [8] Kukina E. G., Roman'kov V. A. *Subquadratic growth of the averaged Dehn function for free Abelian groups* // Siberian Mathematical J., 2003, V. 44, N. 4, P. 605–610.
- [9] Roman'kov V. A. *Asymptotic growth of averaged Dehn functions for nilpotent groups* // Algebra and Logic, 2007, V. 46, N. 1, P. 37–45.
- [10] Gilman R., Myasnikov A., Roman'kov V. *Random equations in nilpotent groups* // J. of Algebra, 2012, V. 352 P. 192–214.
- [11] Gilman R., Myasnikov A., Roman'kov V. *Random equations in free groups* // Groups Complexity Cryptology, 2011, V. 3, P. 257–284.
- [12] Antolin Y., Ciobanu L., Viles N. *On the asymptotics of visible elements and homogeneous equations in surface groups* // Groups, Geometry and Dynamics, 2012, V. 6, P. 619–638.
- [13] Borovik A. V., Myasnikov A. G., Shpilrain V. *Measuring sets in infinite groups* // Computational and Statistical Group Theory, Contemporary Math, Amer. Math. Soc. Providence, RI, 298, P. 21–42.
- [14] Katznelson Y. *Integral Matrices of Fixed Rank* // Proc. Amer. Math. Soc., 1994, V. 120, N. 3, P. 667–675.
- [15] Beck M., Robins S. *Computing the Continuous Discretely* // Springer, 2007.
- [16] Stanley R. *Enumerative combinatorics* // Vol. 1, Cambridge university press, 1997.
- [17] Software package LattE: Lattice-Point Enumeration, Available at <https://www.math.ucdavis.edu/latte/>
- [18] Betke U. McMullen P. *Lattice points in lattice polytopes* // Monatshefte für Mathematik, 1985, V. 99, N. 4, P. 253–265.
- [19] Menshov A. V. *Asymptotic density of rational sets in free abelian groups* // arXiv:math.GR/1401.6558
- [20] Beck M., De Loera J., Develin M., Pfeifle J., Stanley R. *Coefficients and roots of Ehrhart polynomials* In: Integer Points in Polyhedra-Geometry, Number Theory, Algebra, Optimization, volume 374 of Contemp. Math., pages 1536. Amer. Math. Soc., Providence, RI, 2005. arXiv:math.CO/0402148.
- [21] Smith H. J. S. *On Systems of Linear Indeterminate Equations and Congruences* // Philosophical Transactions of the Royal Society of London, 1861, V. 151, P. 293–326.
- [22] Duke W., Rudnick Z., Sarnak P. *Density of integer points on affine homogeneous varieties* // Duke Math Journal, 1993, V. 71, N. 1, P. 143–179.
- [23] Maze G., Rosenthal J., Wagner U. *Natural density of rectangular unimodular integer matrices* // Linear Algebra and Its Applications, 2011, V. 434, N. 5, P. 1319–1324.

INSTITUTE OF MATHEMATICS AND INFORMATION TECHNOLOGIES, OMSK STATE DOS-TOEVSKII UNIVERSITY

E-mail address: menshov.a.v@gmail.com